DOCKET NO.: 272287US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yasuaki HONDA, et al.
SERIAL NO.: NEW U.S. PCT APPLICATION
FILED: HEREWITH
INTERNATIONAL APPLICATION NO.: PCT/JP03/14634
INTERNATIONAL FILING DATE: November 18, 2003
FOR: INFORMATION PROCESSING DEVICE, SERVER CLIENT SYSTEM, METHOD, AND COMPUTER PROGRAM

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119 AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY	APPLICATION NO	DAY/MONTH/YEAR
Japan	2002-339080	22 November 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/14634. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

日本国特許庁
JAPAN PATENT OFFICE

18.11.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月２２日

出願番号
Application Number: 特願２００２－３３９０８０

[ST. 10/C]: [ＪＰ２００２－３３９０８０]

出願人
Applicant(s): ソニー株式会社

２００３年１２月１８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号 出証特２００３－３１０５０３７

【書類名】　特許願

【整理番号】　0290759407

【提出日】　平成14年11月22日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/32

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　本田　康晃

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　吉川　典史

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　五十嵐　卓也

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　小堀　洋一

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　森田　岳彦

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　048747

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

アクセス制御リストの生成処理を実行する情報処理装置であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信部と、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストを格納した記憶部と、

前記受信部における受信パケットに基づくクライアント登録処理に際して、前記ＭＡＣリストの空きスロットの有無を確認し、空きスロットがある場合にのみ登録可能とする判定を行なう登録可否判定部と、

前記登録可否判定部における登録可能の判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理部と、

を有することを特徴とする情報処理装置。

【請求項２】

前記登録処理部は、

前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記情報処理装置は、さらに、

クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析部を有し、

前記登録可否判定部は、クライアントからの受信パケットが登録処理要求パケットである場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

前記登録処理部は、前記登録可否判定部における登録可能の判定に基づく登録

処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】

前記情報処理装置において、

前記登録可否判定部は、クライアントからの受信パケットがデータ処理要求パケットである場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

前記登録処理部は、前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項５】

前記情報処理装置は、さらに、

前記ＭＡＣリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御部を有することを特徴とする請求項１に記載の情報処理装置。

【請求項６】

前記登録可否判定部は、

クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行する構成を有し、

前記登録処理部は、

クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項７】

前記登録可否判定部は、

クライアントからのデータ処理要求において、ＵＰｎＰプロトコルに従ったシ

ーケンス中のコンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたか否かを判定し、

前記登録処理部は、

前記コンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項８】

前記登録処理部は、

クライアントからの受信パケットに格納されたＭＡＣアドレスおよびＭＡＣアドレスと異なる識別情報を取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項９】

前記ＭＡＣアドレスと異なる識別情報は、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項８に記載の情報処理装置。

【請求項１０】

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置であり、

自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行する制御部を有することを特徴とする情報処理装置。

【請求項１１】

前記制御部は、

前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行する構成であることを特徴とする請求項１０に記載の情報処理装置。

【請求項１２】

前記制御部は、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行する構成であることを特徴とする請求項１０に記載の情報処理装置。

【請求項１３】

アクセス要求を受信するサーバと、アクセス要求を実行するクライアントからなるサーバクライアントシステムにおいて、

前記クライアントは、

自己のＭＡＣアドレスをヘッダ情報中に格納したアクセス制御リスト登録処理要求パケットを、情報処理装置の電源オン処理、または特定アプリケーション起動処理を条件として生成し、送信処理を実行する構成を有し、

前記サーバは、

前記クライアントからのアクセス制御リスト登録処理要求パケットを受信し、１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を確認し、空きスロットがある場合にのみ、前記パケットに基づくクライアント情報の、前記ＭＡＣリストに対する登録処理を実行する構成を有する、

ことを特徴とするサーバクライアントシステム。

【請求項１４】

前記サーバは、

前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行する構成であることを特徴とする請求項１３に記載のサーバクライアントシステム。

【請求項１５】

アクセス制御リストの生成処理を実行する情報処理方法であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理ステップと、

を有することを特徴とする情報処理方法。

【請求項１６】

前記登録処理ステップは、

前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項１７】

前記情報処理方法は、さらに、

クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析ステップを有し、

前記登録可否判定ステップは、前記パケット解析ステップにおける解析結果がクライアントからの受信パケットが登録処理要求パケットであると判定された場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項１８】

前記情報処理方法において、

前記登録可否判定ステップは、

クライアントからの受信パケットがデータ処理要求パケットである場合においても、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、

前記登録処理部ステップは、

前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡ

Ｃリストに対する登録処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項１９】

前記情報処理方法は、さらに、

前記ＭＡＣリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御ステップを有することを特徴とする請求項１５に記載の情報処理方法。

【請求項２０】

前記登録可否判定ステップは、

クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行するステップを含み、

前記登録処理ステップは、

クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項２１】

前記登録可否判定ステップは、

クライアントからのデータ処理要求において、ＵＰｎＰプロトコルに従ったシーケンス中のコンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたか否かを判定するステップを含み、

前記登録処理ステップは、

前記コンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項２２】

前記登録処理ステップは、

クライアントからの受信パケットに格納されたＭＡＣアドレスおよびＭＡＣアドレスと異なる識別情報を取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする請求項１５に記載の情報処理方法。

【請求項２３】

前記ＭＡＣアドレスと異なる識別情報は、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする請求項２２に記載の情報処理方法。

【請求項２４】

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法であり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

前記トリガ情報の検出を条件として、自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とする情報処理方法。

【請求項２５】

前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行することを特徴とする請求項２４に記載の情報処理方法。

【請求項２６】

前記パケット生成送信処理ステップは、

前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行することを特徴とする請求項２４に記載の情報処理方法。

【請求項２７】

アクセス制御リストの生成処理を実行するコンピュータプログラムであり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

【請求項２８】

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法を実行するコンピュータプログラムであり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

前記トリガ情報の検出を条件として、自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムに関する。さらに、詳細には、ネットワーク接続された機器間での通信を実行する構成において、ユーザに負担をかけることなく効率的にアクセス権限判定情報を生成し、生成情報に基づくアクセス制限処理を可能

とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

昨今のデータ通信ネットワークの普及に伴い、家庭内においても家電機器やコンピュータ、その他の周辺機器をネットワーク接続し、各機器間での通信を可能とした、いわゆるホームネットワークが浸透しつつある。ホームネットワークは、ネットワーク接続機器間で通信を行なうことにより各機器のデータ処理機能を共有したり、機器間でコンテンツの送受信を行なう等、ユーザに利便性・快適性を提供するものであり、今後、ますます普及することが予測される。

【０００３】

このようなホームネットワークの構成に適するプロトコルとしてユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）が知られている。ユニバーサルプラグアンドプレイ（ＵＰｎＰ）は、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり、困難な操作や設定を伴うことなくネットワーク接続された機器において各接続機器の提供サービスを受領可能とするものである。また、ＵＰｎＰはデバイス上のＯＳ（オペレーティングシステム）にも依存せず、容易に機器の追加ができるという利点を持つ。

【０００４】

ＵＰｎＰは、接続機器間で、ＸＭＬ（eXtensible Markup Language）に準拠した定義ファイルを交換し、機器間において相互認識を行なう。ＵＰｎＰの処理の概要は、以下の通りである。

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

【０００５】

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供および受領が可能となる。ネットワークに新たに接続される機器は、上記のアドレッシング処理によりデバイスＩＤを取得し、ディスカバリ処理によりネットワーク接続された他のデバイスの情報を取得して、取得情報に基づいて他の機器にサービスの要求が可能となる。

【０００６】

しかし、一方、この種のネットワークでは、不正アクセスに対する対策を考慮することも必要となる。ホームネットワーク内の機器、例えばサーバ等には私的なコンテンツや有料コンテンツ等の著作権管理を要求されるコンテンツが格納されることも多い。

【０００７】

このようなホームネットワーク内のサーバに格納されたコンテンツは、ネットワーク接続された他の機器からアクセス可能となる。例えば、上述の簡易な機器接続構成であるＵＰｎＰ接続を実行した機器によってコンテンツを取得することが可能となる。コンテンツが映画データや音楽データの場合、ネットワーク接続機器としてＴＶ、あるいはプレーヤ等を接続すれば、映画を視聴したり、音楽を聴いたりすることが可能となる。

【０００８】

コンテンツの利用権を有するユーザの接続した機器によるアクセスは許容されてもよいが、上述のようなネットワーク構成においては、コンテンツ等の利用権を持たないユーザがネットワークに入り込むことも容易である。例えば無線ＬＡＮによって構成されたネットワークの場合には家の中にあるサーバに対して、戸外、あるいは隣家等から通信機器を利用して不正にネットワークに参入し、コンテンツの搾取を行なうような事態も発生し得る。このような不正なアクセスを許容する構成は、秘密漏洩を生じさせることにもなり、また、コンテンツ著作権の管理の観点からも重要な問題となる。

【０００９】

上述のような不正アクセスを排除するため、例えばサーバにアクセスを許容するクライアントのリストを保持させ、クライアントからサーバに対するアクセス

要求の際に、サーバでリストとの照合処理を実行して不正アクセスを排除する構成が提案されている。

【００１０】

例えば、ネットワーク接続機器に固有の物理アドレスであるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを、アクセス許容機器リストとして設定するＭＡＣアドレスフィルタリングが知られている。ＭＡＣアドレスフィルタリングとは、ホームネットワーク等の内部ネットワーク（サブネット）と外部ネットワークとを隔離するルータあるいはゲートウェイに、予めアクセスを許容するＭＡＣアドレスを登録しておき、受信したパケットのＭＡＣアドレスと登録されたＭＡＣアドレスとを照合し、登録されていないＭＡＣアドレスを有する機器からのアクセスを拒否するものである。なお、この種の技術については、例えば特許文献１に開示されている。

【００１１】

しかし、アクセス制限をするためのＭＡＣアドレスの登録処理を行なうためには、ネットワークに接続される機器の全てのＭＡＣアドレスを調べることが必要であり、取得した全ての機器のＭＡＣアドレス（４８ｂｉｔ）をオペレータが入力してリストを作成するという処理が必要となる。このような処理は、例えば特定の会社、団体等、セキュアな環境を構築することが要求される場合には、所定の管理者の下に行なうことも可能であるが、例えば一般家庭に設定されるホームネットワーク環境において、一般ユーザにＭＡＣリストの生成、格納を要求することは現実的ではない。

【００１２】

ホームネットワークにおいては、新たな機器の追加処理が行われることは頻繁に発生することであり、このような機器追加処理の際に、ユーザが逐次、機器のＭＡＣアドレスを調べて登録処理をしなければならないとすると、ネットワーク構築の容易性を阻害することになる。

【００１３】

一方、一般家庭においても、ＰＣのみならず、家電機器も含んだネットワーク構成が構築され、どのような機器からでもネットワークにアクセス可能ないわゆ

るユビキタス環境が構築されつつあり、また、無線ＬＡＮ等の普及により、通信可能な機器が外部から無線ＬＡＮに侵入することも容易となっている。このようなネットワーク環境において、ネットワーク接続機器に対する不正アクセスもより発生しやすくなっており、不正なアクセスによる秘密情報の搾取、コンテンツの不正読み取り等が実行される可能性はますます高くなっている。このような状況において、一般ユーザに負担を強いることなく、適切なアクセス制御構成を容易に実現することが求められている。

【００１４】

【特許文献１】

特許公開平１０－２７１１５４号公報

【００１５】

【発明が解決しようとする課題】

本発明は、上述の問題点に鑑みてなされたものであり、様々な機器がネットワーク接続される構成において、ネットワーク接続機器を有するユーザに負担を強いることなく、容易にかつ的確にアクセス制御構成を構築することを可能とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１６】

本発明は、例えば、ネットワーク接続された様々な機器（クライアント）からの処理要求を受信する機器（サーバ）において、クライアント識別により処理要求権限を有するか否かを判断し、処理要求権限のあるクライアントからの要求に対してのみサーバが処理要求に応じる構成を実現し、不正な機器からの処理要求を排除することで秘密漏洩を防止するとともに、コンテンツ著作権についても適正な管理を実現することを可能とした情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１７】

【課題を解決するための手段】

本発明の第１の側面は、

アクセス制御リストの生成処理を実行する情報処理装置であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信部と、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストを格納した記憶部と、

前記受信部における受信パケットに基づくクライアント登録処理に際して、前記ＭＡＣリストの空きスロットの有無を確認し、空きスロットがある場合にのみ登録可能とする判定を行なう登録可否判定部と、

前記登録可否判定部における登録可能の判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理部と、

を有することを特徴とする情報処理装置にある。

【００１８】

さらに、本発明の情報処理装置の一実施態様において、前記登録処理部は、前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行する構成であることを特徴とする。

【００１９】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析部を有し、前記登録可否判定部は、クライアントからの受信パケットが登録処理要求パケットである場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部は、前記登録可否判定部における登録可能の判定に基づく登録処理を実行する構成であることを特徴とする。

【００２０】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置において、前記登録可否判定部は、クライアントからの受信パケットがデータ処理要求パケットである場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部は、前記登録可否判定部における

登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする。

【００２１】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、さらに、前記ＭＡＣリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御部を有することを特徴とする。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記登録可否判定部は、クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行する構成を有し、前記登録処理部は、クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする。

【００２３】

さらに、本発明の情報処理装置の一実施態様において、前記登録可否判定部は、クライアントからのデータ処理要求において、ＵＰｎＰプロトコルに従ったシーケンス中のコンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたか否かを判定し、前記登録処理部は、前記コンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する構成であることを特徴とする。

【００２４】

さらに、本発明の情報処理装置の一実施態様において、前記登録処理部は、クライアントからの受信パケットに格納されたＭＡＣアドレスおよびＭＡＣアドレスと異なる識別情報を取得し、前記ＭＡＣリストに対する登録処理を実行する構

成であることを特徴とする。

【００２５】

さらに、本発明の情報処理装置の一実施態様において、前記ＭＡＣアドレスと異なる識別情報は、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする。

【００２６】

さらに、本発明の第２の側面は、

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置であり、

自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行する制御部を有することを特徴とする情報処理装置にある。

【００２７】

さらに、本発明の情報処理装置の一実施態様において、前記制御部は、前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行する構成であることを特徴とする。

【００２８】

さらに、本発明の情報処理装置の一実施態様において、前記制御部は、前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行する構成であることを特徴とする。

【００２９】

さらに、本発明の第３の側面は、

アクセス要求を受信するサーバと、アクセス要求を実行するクライアントからなるサーバクライアントシステムにおいて、

前記クライアントは、

自己のＭＡＣアドレスをヘッダ情報中に格納したアクセス制御リスト登録処理要求パケットを、情報処理装置の電源オン処理、または特定アプリケーション起

動処理を条件として生成し、送信処理を実行する構成を有し、

前記サーバは、

前記クライアントからのアクセス制御リスト登録処理要求パケットを受信し、１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を確認し、空きスロットがある場合にのみ、前記パケットに基づくクライアント情報の、前記ＭＡＣリストに対する登録処理を実行する構成を有する、

ことを特徴とするサーバクライアントシステムにある。

【００３０】

さらに、本発明のサーバクライアントシステムの一実施態様において、前記サーバは、前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行する構成であることを特徴とする。

【００３１】

さらに、本発明の第４の側面は、

アクセス制御リストの生成処理を実行する情報処理方法であり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理ステップと、

を有することを特徴とする情報処理方法にある。

【００３２】

さらに、本発明の情報処理方法の一実施態様において、前記登録処理ステップは、前記クライアントからの受信パケットのヘッダ部に含まれる送信元ＭＡＣアドレスを取得し、前記ＭＡＣリストに対する登録情報として適用する処理を実行

することを特徴とする。

【００３３】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、クライアントからの受信パケットが登録処理要求パケットであるかデータ処理要求であるかを判別するパケット解析ステップを有し、前記登録可否判定ステップは、前記パケット解析ステップにおける解析結果がクライアントからの受信パケットが登録処理要求パケットであると判定された場合に、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行することを特徴とする。

【００３４】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法において、前記登録可否判定ステップは、クライアントからの受信パケットがデータ処理要求パケットである場合においても、前記ＭＡＣリストの空きスロット有無検出処理に基づく登録可否判定処理を実行し、前記登録処理部ステップは、前記登録可否判定部における登録可能の判定に基づいて、受信したデータ処理要求パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする。

【００３５】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、前記ＭＡＣリストの空きスロットの設定処理からの経過時間が予め定められた閾値時間を経過したことを条件として、空きスロットのクローズ処理を実行する制御ステップを有することを特徴とする。

【００３６】

さらに、本発明の情報処理方法の一実施態様において、前記登録可否判定ステップは、クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているか否かを判定する処理を実行するステップを含み、前記登録処理ステップは、クライアントからのデータ処理要求シーケンスが、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行しているとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレ

スを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする。

【００３７】

さらに、本発明の情報処理方法の一実施態様において、前記登録可否判定ステップは、クライアントからのデータ処理要求において、ＵＰｎＰプロトコルに従ったシーケンス中のコンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたか否かを判定するステップを含み、前記登録処理ステップは、前記コンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されたとの判定に基づいて、クライアントからの受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする。

【００３８】

さらに、本発明の情報処理方法の一実施態様において、前記登録処理ステップは、クライアントからの受信パケットに格納されたＭＡＣアドレスおよびＭＡＣアドレスと異なる識別情報を取得し、前記ＭＡＣリストに対する登録処理を実行することを特徴とする。

【００３９】

さらに、本発明の情報処理方法の一実施態様において、前記ＭＡＣアドレスと異なる識別情報は、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報であることを特徴とする。

【００４０】

さらに、本発明の第５の側面は、

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法であり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ情報として検出するトリガ検出ステップと、

前記トリガ情報の検出を条件として、自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とする情報処理方法にある。

【００４１】

さらに、本発明の情報処理方法の一実施態様において、前記パケット生成送信処理ステップは、前記アクセス制御リスト登録処理要求パケットの生成処理において、グローバルユニークなＩＤ情報、またはクライアント機器に設定された鍵情報からなる識別情報を格納したパケット生成処理を実行することを特徴とする。

【００４２】

さらに、本発明の情報処理方法の一実施態様において、前記パケット生成送信処理ステップは、前記アクセス制御リスト登録処理要求パケットをブロードキャスト送信またはマルチキャスト送信として実行することを特徴とする。

【００４３】

さらに、本発明の第６の側面は、

アクセス制御リストの生成処理を実行するコンピュータプログラムであり、

アクセス要求機器としてのクライアントからのパケットを受信する受信ステップと、

１つのクライアントのＭＡＣアドレスを含む情報を１つのスロットの登録データとして設定したＭＡＣリストの空きスロットの有無を判定する登録可否判定ステップと、

前記登録可否判定ステップにおける空きスロット有りの判定に基づいて、前記受信パケットからクライアントＭＡＣアドレスを含むデータを取得し、前記ＭＡＣリストに対する登録処理を実行する登録処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００４４】

さらに、本発明の第７の側面は、

ネットワーク接続されたサーバに対するアクセス要求を実行するクライアントとしての情報処理装置における情報処理方法を実行するコンピュータプログラムであり、

情報処理装置の電源オン処理、または特定アプリケーション起動処理をトリガ

情報として検出するトリガ検出ステップと、

前記トリガ情報の検出を条件として、自己のＭＡＣアドレスをヘッダ情報中に格納し、前記サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して送信する処理を実行するパケット生成送信処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００４５】

【作用】

本発明の構成によれば、ネットワークに接続されたクライアント機器の電源をＯＮとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとして、ＭＡＣリスト登録処理要求パケットを自動送信し、サーバ側で、ＭＡＣリストの空きスロットの状況に応じて、受信パケットからＭＡＣアドレス等の情報を取得して登録する処理を実行する構成としたので、ユーザの負担を発生させることなくアクセス制御リストとしてのＭＡＣリストが容易に、かつ効率的に生成可能となる。

【００４６】

また、本発明の構成によれば、サーバにＭＡＣリストの空きスロットを設定した後、閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、ＭＡＣリスト中の空きスロットのクローズ処理を実行する構成としたので、ＭＡＣリストの空きスロットを放置することがなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

【００４７】

さらに、本発明の構成によれば、クライアントから受信する通常のデータ処理要求に応じてサーバ側で未登録のクライアントを登録する処理を実行する構成としたので、登録処理要求パケットを適用することなくＭＡＣリストへのクライアント登録が可能となる。

【００４８】

さらに、本発明の構成によれば、クライアントが、特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器であり、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行している場合には、ＭＡＣリストへの自動登録が可能となり、ユーザの負担を発生させることのないＭＡＣリスト生成が可能となる。

【００４９】

さらに、本発明の構成によれば、ＭＡＣリストの登録情報としてグローバルユニークな識別子としてのＧＵＩＤや、機器に対して設定された固有の鍵情報データを格納し、データ処理要求を受信したサーバが、ＭＡＣアドレスのみならず、ＧＵＩＤや鍵情報等の識別データを用いてクライアント確認を実行することが可能となり、高いレベルでのセキュリティ管理が実現される。

【００５０】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００５１】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００５２】

【発明の実施の形態】

以下、図面を参照しながら、本発明の情報処理装置、サーバクライアントシステム、および方法、並びにコンピュータ・プログラムの詳細について説明する。

【００５３】

［システム概要およびＭＡＣリスト］

まず、図１を参照して、本発明の適用可能なネットワーク構成例について説明する。図１は、様々なクライアント機器からの処理要求に応じて処理を実行するサーバ１０１と、サーバ１０１に対して処理要求を行なうクライアント機器としてのＰＣ１２１，１２２，１２４、ＰＤＡ、携帯電話等の携帯通信端末１２３，１２５がネットワーク１００を介して接続された構成、例えばホームネットワーク構成を示している。

【００５４】

サーバ１０１がクライアントからの要求に応じて実行する処理は、例えばサーバ１０１の保有するハードディスク等の記憶手段に格納されたコンテンツの提供、あるいはサーバの実行可能なアプリケーションプログラムの実行によるデータ処理サービス等である。なお、図１においては、サーバ１０１と、その他のクライアント機器としてのＰＣ１２１，１２２，１２４、ＰＤＡ、携帯電話等の携帯通信端末１２３，１２５とを区別して示しているが、クライアントからの要求に対するサービスを提供する機器をサーバとして示しているものであり、いずれのクライアント機器も、自己のデータ処理サービスを他のクライアントに提供する場合には、サーバとしての機能を提供可能となる。従って、図１に示すネットワーク接続されたクライアント機器もサーバとなり得る。

【００５５】

ネットワーク１００は、有線、無線等いずれかのネットワークであり、各接続機器は、ＭＡＣ(Media Access Control)アドレスを有している。各ネットワーク接続機器は、宛先ＭＡＣアドレスおよび送信元ＭＡＣアドレスをヘッダ情報に持つパケット、例えばイーサネット（登録商標）フレームをネットワーク１００を介して送受信する。すなわち、クライアントは、イーサネットフレームのデータ部に処理要求情報を格納したフレームをサーバ１０１に送信することにより、サーバ１０１に対するデータ処理要求を実行する。サーバ１０１は、処理要求フレームの受信に応じて、後述するアクセス権限判定処理を行ない、権限ありの判定を条件としてデータ処理を実行し、必要に応じてデータ処理結果としての結果データをイーサネットフレームのデータ部に格納し、各クライアントに送信する。

【００５６】

ネットワーク接続機器は、例えばユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器によって構成される。従って、ネットワークに対する接続機器の追加、削除が容易な構成である。ネットワークに新たに接続する機器は、

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理。

上記処理手順を行なうことで、ネットワーク接続された機器を適用したサービスを受領することが可能となる。

【００５７】

図１に示すサーバおよびクライアント機器を構成するＰＣ等の情報処理装置のハードウェア構成例について図２を参照して説明する。

【００５８】

ＣＰＵ(Central Processing Unit)３０１は、ＲＯＭ(Read Only Memory)３０２、またはＨＤＤ３０４等に記憶されているプログラムに従って、各種の処理を実行し、データ処理手段、あるいは通信制御処理手段として機能する。ＲＡＭ３０３には、ＣＰＵ３０１が実行するプログラムやデータが適宜記憶される。ＣＰＵ３０１、ＲＯＭ３０２、およびＲＡＭ３０３、ＨＤＤ３０４は、バス３０５を介して相互に接続されている。

【００５９】

バス３０５には、入出力インタフェース３０６が接続されており、この入出力インタフェース３０６には、例えば、ユーザにより操作されるキーボード、スイッチ、ボテン、あるいはマウス等により構成される入力部３０７、ユーザに各種の情報を提示するＬＣＤ、ＣＲＴ、スピーカ等により構成される出力部３０８が接続される。さらに、データ送受信手段として機能する通信部３０９、さらに、

磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリなどのリムーバブル記録媒体３１１を装着可能で、これらのリムーバブル記録媒体３１１からのデータ読み出しあるいは書き込み処理を実行するドライブ３１０が接続される。

【００６０】

図２に示す構成は、図１に示すネットワーク接続機器の一例としてのサーバ、パーソナルコンピュータ（ＰＣ）の例であるが、ネットワーク接続機器はＰＣに限らず、図１に示すように携帯電話、ＰＤＡ等の携帯通信端末、その他の様々な電子機器、情報処理装置によって構成することが可能である。従って、それぞれの機器固有のハードウェア構成を持つことが可能であり、そのハードウェアに従った処理を実行する。

【００６１】

本発明において、アクセス制御を行なうネットワーク接続機器は、アクセス権限を有するネットワーク接続機器の機器リストとしてアクセス権限を有するネットワーク接続機器のＭＡＣアドレスを登録したＭＡＣリストを生成し、格納する。従来においても、ＭＡＣリストに基づくアクセス制限構成は存在するが、これは、ユーザが、各ネットワーク接続機器のＭＡＣアドレスを調べ、調べたＭＡＣアドレスを入力してリストを作成する処理を必要としていた。

【００６２】

本発明の構成においては、このようなユーザによる処理を行なうことは必要ではなく、アクセス制御を行なうネットワーク接続機器が、ネットワーク接続機器からのパケット受信に基づいて自動的にＭＡＣリストを作成する。

【００６３】

図３に、アクセス制御を実行するネットワーク接続機器（サーバ）の処理機能を説明するブロック図を示す。サーバは、ネットワークを介したパケットの送受信を実行するパケット送受信部５０１、パケット送受信部５０１を介して受信するパケットの解析および、パケット送受信部５０１を介して送信するパケットを生成するパケット生成、解析部５０２、クライアントから受信するパケットに基づいてＭＡＣリストに対する登録可否を判定する登録可否判定部５０３、登録可

否判定部５０３の判定に基づいて登録処理を実行する登録処理部５０４、ＭＡＣリストを格納した記憶部５０５、さらに、サーバに対する様々なデータ処理要求パケットに基づいて、データ処理要求クライアントがＭＡＣリストに登録されているか否かに基づいてデータ処理の実行可否を判定するデータ処理可否判定部５０６、データ処理可否判定部におけるデータ処理可の判定を条件として、クライアントの要求するデータ処理を実行するデータ処理部５０７を有する。

【００６４】

図４に、アクセス制御を実行するネットワーク接続機器（サーバ）に格納されるアクセス制御リストとしてのＭＡＣリストの構成例を示す。

【００６５】

ＭＡＣリストは、サーバ内の記憶部（不揮発性メモリ）に格納される。ＭＡＣリストは、スロット単位で、各クライアントの登録データを格納する構成を有し、１スロット毎に１つの登録クライアント情報を格納する。

【００６６】

登録情報には、クライアントのＭＡＣアドレス、ユーザが任意に設定可能なクライアント名、登録日時が含まれる。さらに、オプションとして、ＭＡＣアドレスとは異なる識別データ、例えばＧＵＩＤ（Global Unique Identifier）等の固有識別子、あるいは各クライアント機器に設定された鍵データ等を格納してもよい。これらの格納データは、登録処理の際にクライアントから送信されるパケット（イーサネットフレーム）に含まれるデータであり、サーバは、クライアントからの送信パケット（イーサネットフレーム）から登録情報を取得してＭＡＣリストに対する登録処理を実行する。

【００６７】

イーサネットフレームの構成を図５に示す。イーサネットフレームは、ヘッダ部、データ部、トレーラ部に区分され、ヘッダ部には、同期信号、パケット開始符号、宛先ＭＡＣアドレス、送信元ＭＡＣアドレス、およびパケット長，タイプが含まれる。

【００６８】

データ部には、例えばＴＣＰ／ＩＰ通信プロトコルに従って生成されたデータ

が含まれ、例えば送信元、送信先ＩＰアドレスを含むＩＰパケットが格納される。図４に示すＭＡＣリストの登録データ中、ＭＡＣアドレス情報は、図５に示すイーサネットフレームのヘッダ部に設定される送信元ＭＡＣアドレスから取得し、その他の情報は、データ部の格納データから取得する。これらの情報を登録処理を実行するサーバ、すなわち、イーサネットフレーム（パケット）を受信したサーバが取得して、パケットから必要情報を読み出して、ＭＡＣリストに対する登録処理を実行する。

【００６９】

図４に示すＭＡＣリストは、前述したようにスロット単位で１クライアント情報が格納される。スロット数はユーザが任意に設定可能である。サーバにおいて、クライアント情報を登録する際には、空きスロットがあるか否かを判断し、空きスロットがある場合に限り新規登録が可能となる。図４に示す例では、設定スロット数は、＃０１～＃０３の３つであり、スロットＮｏ．＃０４～は、クローズ状態であるので、最大３つのクライアントを登録可能とした状態を示している。

【００７０】

ユーザは新規のクライアントをネットワークに接続して登録処理を実行する際には、サーバのＭＡＣリストに空きスロットを生成する。図４に示す状態は、スロットＮｏ．＃０１，＃０２が登録済みスロットであり、スロットＮｏ．＃０３が空きスロットとして設定され、スロットＮｏ．＃０３に対して、１つのクライアントのみ新規登録可能な状態である。なお、空きスロットを設定した後、空きスロットは所定時間後に自動的にクローズされる構成としてもよい。これは、ユーザの予期しない第三者の機器による不正登録の発生を防止するためである。これらの処理については、後述する。

【００７１】

[ＭＡＣリストに対するクライアント登録処理]

次に、クライアントのＭＡＣリストに対する登録処理手順の基本シーケンスについて、図６の処理フローを用いて説明する。

【００７２】

左側がＭＡＣリストに対する登録要求を実行するクライアントの処理を示しており、右側がクライアントからの登録要求を受信しＭＡＣリストに対する登録処理を実行するサーバ側の処理を示している。

【００７３】

クライアントは、ステップＳ１１１において、機器の電源をＯＮとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理を実行すると、ステップＳ１１２において、これらの処理をトリガとして登録処理要求パケットをサーバに対して自動送信する。なお、このパケット送信は、ブロードキャストあるいはマルチキャスト送信として実行される。

【００７４】

すなわち、クライアントとしての情報処理装置は、制御部、すなわち、図２のハードウェア構成例のＣＰＵ３０１が、記憶部に格納されたプログラムに従って、機器の電源をＯＮとする処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理を検出し、該検出情報をトリガとして登録処理要求パケット、すなわち、ヘッダにＭＡＣアドレスを格納し、サーバの保有するＭＡＣリストに対する登録要求であることを明示したアクセス制御リスト登録処理要求パケットを生成して、サーバに対して自動送信する処理を実行する。

【００７５】

図７に登録要求の際に送信されるメッセージデータのデータ部の主要構成例を示す。「Ｂ－ＰＯＳＴ＊ＨＴＴＰ／１．１」は、メッセージの書式がＨＴＴＰのＶｅｒ．１．１であることを示し、「ＨＯＳＴ：１９２．２５４．２５５．２５５：３５３６」は、ブロードキャスト用のホストのＩＰアドレスと、ポート番号を示す。「Ｃｏｎｔｅｎｔ－Ｔｙｐｅ：ａｐｐｌｉｃａｔｉｏｎ／．．．」、「Ｃｏｎｔｅｎｔ－Ｌｅｎｇｔｈ：６５」は、コンテンツタイプおよびレングスを示し、「Ｂｒｏａｄｃａｓｔ　ＳＮＡＣ」は、ある特定のネットワークアクセスコントロール（ＳＮＡＣ）に従った、ブロードキャスト送信であることを示し、「Ｍｅｔｈｏｄ：Ｒｅｇｉｓｔｅｒ」は、本パケットに従って実行すべき実行メ

ソッドが登録メソッドであることを示している。

【００７６】

さらに、上記データに加え、図４のＭＡＣリストの登録データとして含まれるクライアント名、ＧＵＩＤ等のＩＤ情報、鍵情報等を含める構成としてもよい。登録処理の際に送信するパケットに格納するデータは、サーバ側のＭＡＣリストに何を登録するかに応じて定義することが可能であり、クライアントは、電源ＯＮ時、あるいはホームネットワークを利用したサービスの実行アプリケーションの起動時に、定義情報に従ったデータを格納した登録処理要求パケットを生成し、送信する処理を実行する。

【００７７】

図６の処理フローに戻りＭＡＣリストに対するクライアント情報登録シーケンスについて説明を続ける。ステップＳ１２１において、クライアントから上述したデータを含む登録処理要求パケットを、図３に示すパケット送受信部５０１を介して受信し、パケット生成、解析部５０２において、パケット解析を実行し、登録処理要求パケットであることを判別し、登録可否判定部５０３において登録可否の判定を実行する。

【００７８】

サーバは、ステップＳ１２２において、自己の記憶部５０５内のＭＡＣリストを参照し、受信パケットに含まれる送信元ＭＡＣアドレスに対応するデータが既に登録済みか否かを判定し、登録済みであれば、処理を終了する。なお、この際、登録済みであることを通知する応答メッセージをクライアント側に送信する処理を実行する構成としてもよい。

【００７９】

ステップＳ１２２において、自己の記憶部５０５内のＭＡＣリストに、受信パケットに含まれる送信元ＭＡＣアドレスに対応するデータが登録されていないと判定した場合は、ステップＳ１２３において、ＭＡＣリストにデータ登録可能な空きスロットが存在するか否かを判定する。空きスロットが無い場合は、新規クライアントの登録処理は実行できないので、処理を終了する。なお、この際、登録不可であることを通知する応答メッセージをクライアント側に送信する処理を

実行する構成としてもよい。

【００８０】

ステップＳ１２３において、ＭＡＣリストにデータ登録可能な空きスロットが存在すると判定された場合には、ステップＳ１２４において、図３に示す登録処理部５０４が、クライアントから受信した登録処理要求パケットのヘダに含まれる送信元ＭＡＣアドレスおよびデータ部に含まれる登録情報を取得し、ＭＡＣリストの空きスロットに登録する処理を実行する。

【００８１】

以上の処理によって、サーバによるクライアントのＭＡＣリストへの登録処理が終了する。ＭＡＣリストに登録されたクライアントは、サーバに対するデータ処理要求を、先に説明したイーサネットフレーム（図５参照）等のパケットによりサーバに送信すると、サーバのデータ処理可否判定部５０６（図３参照）ではイーサネットフレームのヘッダ情報から送信元ＭＡＣアドレスを取得し、記憶部５０５に格納されたＭＡＣリストの登録情報との照合を実行し、登録されたＭＡＣアドレスと一致した場合は、データ処理部５０７において要求処理を実行、例えばコンテンツの提供等を実行する。

【００８２】

クライアントから受信したデータ処理要求フレームのヘッダ情報中の送信元ＭＡＣアドレスが、記憶部５０５に格納されたＭＡＣリストに登録されていない場合は、不正なクライアントからの処理要求であると判定し、クライアントの要求処理は実行しない。

【００８３】

なお、図６を参照して説明したＭＡＣリストに対するクライアント情報の登録処理は、基本的にスロットに空きスロットがあれば自動登録する処理として説明したが、登録の可否をユーザ自身が判定した後、ＭＡＣリストに対する登録処理を実行する構成としてもよい。この場合、図６の処理ステップのステップＳ１２３とステップＳ１２４の間で、ユーザによる判定処理ステップを実行することになる。例えば、サーバが受信したパケット情報をディスプレイに表示し、ユーザが表示情報に基づいて、登録可と判定した場合にのみ、入力手段から登録実行コ

マンドを入力し、ユーザ入力を条件としてＭＡＣリストに対する登録を行なう。このような構成によれば、さらにセキュアな登録処理が可能となる。

【００８４】

[空きスロットの自動クローズ処理]

次に、ＭＡＣリストを格納したサーバにおいて実行されるＭＡＣリスト中の空きスロット設定およびスロットのクローズ処理について説明する。前述したように、ＭＡＣリストはサーバの記憶部にスロット単位で設定され、各スロットに１つのクライアント情報が格納される。

【００８５】

空きスロットの設定、空きスロットのクローズ処理はユーザによる処理によって実行可能である。ただし、空きスロットを設定した後、長時間、空きスロットを放置した場合、上述したユーザ確認を伴わない自動登録処理を実行すると、第三者による不正な登録処理が行われる可能性がある。このような事態を防止するため、設定された空きスロットを予め定められた閾値時間経過後、自動的にクローズする処理を実行する。すなわち、ＭＡＣリストを保持するサーバの制御部は、ＭＡＣリストに設定される空きスロット設定からの経過時間を計測し、計測時間が予め設定された閾値時間を経過したことを条件としてクローズ処理を実行する。

【００８６】

空きスロットの設定および自動クローズ処理について、図８のフローを参照して説明する。ステップＳ２０１において、ユーザによりＭＡＣリストに空きスロットの設定がなされる。通常、ユーザは新たなクライアント機器をネットワークに接続する際、新規接続機器の数に応じて空きスロットを追加設定する。このように必要な数のみのスロットを設定し、不要な空きスロットを設定しないことで、ユーザの管理する機器のみをＭＡＣリストに登録することができる。

【００８７】

ステップＳ２０１の空きスロット設定の後、サーバは、登録処理要求パケットを待機する。これは、図６のフローを参照して説明したクライアントからの登録処理要求パケットであり、例えばクライアントの電源ＯＮまたは、アプリケーシ

ョン起動に応じて自動送信されるパケットである。

【００８８】

サーバは、ステップＳ２０１の空きスロットの設定からの経過時間を計測し、ステップＳ２０３において予め定めた閾値時間との比較を行なう。ステップＳ２０４において、閾値時間内にクライアントからの登録処理要求パケットを受信した場合は、ステップＳ２０５において登録処理要求パケットからＭＡＣアドレス等の登録情報を取得してＭＡＣリストの空きスロットに対する登録処理を実行する。

【００８９】

閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、ステップＳ２０６に進み、ＭＡＣリスト中の空きスロットのクローズ処理を実行する。このクローズ処理により、ＭＡＣリストには空きスロットが存在しなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

【００９０】

[データ処理要求時の登録処理]

先に図６を参照して説明した新規クライアントのＭＡＣリストに対する登録処理は、登録要求を示す登録処理要求パケットをサーバが受信した場合に実行する登録処理であったが、このような明示的な登録要求に応じてＭＡＣリストに対する処理を実行するのみならず、通常のデータ処理要求、例えばサーバの記憶手段に格納した映像データあるいは音楽データ等のコンテンツ取得要求パケットをクライアントから受信した際に、サーバ側でクライアントのＭＡＣリストに対する自動登録を行なう構成も可能である。

【００９１】

以下、図９のフローを参照して、サーバがクライアントから受信する通常のデータ処理要求に基づいて、データ処理要求クライアントをＭＡＣリストへ登録する処理手順について説明する。

【００９２】

まず、ステップＳ３０１において、サーバは、クライアントからの登録処理要求パケットまたはデータ処理要求パケットを受信すると、ステップＳ３０２において、受信パケットが登録処理要求パケットであるか、データ処理要求パケットであるかを判定する。

【００９３】

登録処理要求パケットである場合には、ステップＳ３０３においてＭＡＣリストの空きスロットの有無を判定し、空きスロットのある場合には受信パケットから登録情報を取得して登録処理を行なう。これは図６を参照して説明した処理に相当する。

【００９４】

一方、ステップＳ３０２のパケット種別判定処理において、データ処理要求パケットであると判定した場合には、ステップＳ３０５において、データ処理要求パケットのヘッダ情報に含まれる送信元ＭＡＣアドレスが記憶部に格納したＭＡＣリストに登録済みか否かを判定する。この処理は、図３に示すデータ処理可否判定部５０６において実行する。

【００９５】

ＭＡＣリストに登録済みであれば、登録されたクライアントからのデータ処理要求であるので、ステップＳ３０６において、要求に従った処理を実行する。データ処理は、図３に示すデータ処理部５０７において実行する。

【００９６】

ステップＳ３０５において、データ処理要求パケットのヘッダ情報に含まれる送信元ＭＡＣアドレスが記憶部に格納したＭＡＣリストに登録されていないと判定した場合は、ステップＳ３０７において、ＭＡＣリストの空きスロットの有無を判定し、空きスロットがある場合には、ステップＳ３０８において受信パケットから送信元ＭＡＣアドレス等の登録情報を取得して登録処理を行なう。さらに、登録の後、ステップＳ３０６において、クライアントの要求処理を実行して処理を終了する。

【００９７】

このように、クライアントから受信する通常のデータ処理要求に応じてサーバ

側で未登録のクライアントを登録する処理を実行する構成によれば、特別な登録処理要求パケットの送受信処理を必要とすることなくＭＡＣリストへのクライアント登録が可能となる。

【００９８】

なお、図９を参照して説明したＭＡＣリストに対するクライアント情報の登録処理は、基本的にスロットに空きスロットがあれば自動登録する処理として説明したが、この処理においても先に説明した図６の登録処理要求パケットに対する処理と同様、登録の可否をユーザ自身が判定した後、ＭＡＣリストに対する登録処理を実行する構成としてもよい。この場合、図９の処理ステップのステップＳ３０７とステップＳ３０８の間にユーザによる判定処理ステップを実行することになる。例えば、サーバが受信したパケット情報をディスプレイに表示し、ユーザが表示情報に基づいて、登録可と判定した場合にのみ、入力手段から登録実行コマンドを入力し、ユーザ入力を条件としてＭＡＣリストに対する登録を行なう。このような構成によれば、さらにセキュアな登録処理が可能となる。

【００９９】

[ＵＰｎＰプロトコルに対応するパケットに対する登録処理]

上述したクライアントからの登録処理要求パケットまたはデータ処理要求パケットに基づくサーバにおけるＭＡＣリストへの登録処理を実行する場合には、クライアントからの登録処理要求パケットまたはデータ処理要求パケットが、ある特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットであることを、サーバにおいて認識することが必要となる。従って、このような特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットを送信できない機器については、上述した受信パケットに基づくＭＡＣリストに対する登録処理ができないことになる。

【０１００】

前述したように、ホームネットワーク等においては、簡易な機器のネットワーク接続を可能としたユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器が接続されることが多く、ＵＰｎＰ対応機器は、様々なメーカにおいて製造されており、既に多くの機器が実在する。

【０１０１】

そこで、特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットを送信できないＵＰｎＰ対応機器についてもＭＡＣリストへの自動登録を可能とする構成例について、以下説明する。

【０１０２】

本実施例は、サーバが、クライアントから受信するパケットに基づいて実行する処理を解析し、ＵＰｎＰプロトコルに従ったシーケンスが的確に実行されているか否かを判定する。ＵＰｎＰプロトコルに従ったシーケンスが的確に実行されているとの判定を条件として、そのＵＰｎＰ対応機器をＭＡＣリストへ登録する処理を実行する。

【０１０３】

図１０に本実施例に従ったサーバの処理シーケンスを説明するフローチャートを示す。サーバは、ステップＳ４０１においてクライアントから処理要求パケットを受信し、ステップＳ４０２において、ＵＰｎＰプロトコルに従った処理シーケンスが的確に実行されているか否かを判定する。

【０１０４】

前述したように、ＵＰｎＰプロトコルに従った処理シーケンスは、基本的に下記ステップから構成される。

（１）ＩＰアドレス等の自己のデバイスＩＤを取得するアドレッシング処理ステップ。

（２）ネットワーク上の各デバイスの検索を行ない、各デバイスから応答を受信し、応答に含まれるデバイス種別、機能等の情報を取得するディスカバリ処理ステップ。

（３）ディスカバリ処理で取得した情報に基づいて、各デバイスにサービスを要求するサービス要求処理ステップ。

【０１０５】

サーバは、上述の処理ステップが的確に実行されていれば、正当なＵＰｎＰ対応のクライアント機器であると判断し、ＭＡＣリストへの登録可能機器であると判定する。上記（１）～（３）の処理が実行されない場合には、登録不可と判定

（Ｓ４０２：Ｎｏ）し、処理を終了する。

【０１０６】

上述の処理ステップが的確に実行されており、正当なＵＰｎＰ対応のクライアント機器であると判定した場合は、ステップＳ４０３において、データ処理要求パケットのヘッダ情報に含まれる送信元ＭＡＣアドレスが記憶部に格納したＭＡＣリストに登録済みか否かを判定する。この処理は、図３に示すデータ処理可否判定部５０６において実行する。

【０１０７】

ＭＡＣリストに登録済みであれば、登録されたクライアントからのデータ処理要求であるので、ステップＳ４０６において、要求に従った処理を実行する。データ処理は、図３に示すデータ処理部５０７において実行する。

【０１０８】

ステップＳ４０３において、データ処理要求パケットのヘッダ情報に含まれる送信元ＭＡＣアドレスが記憶部に格納したＭＡＣリストに登録されていないと判定した場合は、ステップＳ４０４において、ＭＡＣリストの空きスロットの有無を判定し、空きスロットがある場合には、ステップＳ４０５において受信パケットから登録情報を取得して登録処理を行なう。さらに、登録の後、ステップＳ４０６において、クライアントの要求処理を実行して処理を終了する。

【０１０９】

このように、本実施例に従えば、クライアントが、特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器であり、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行している場合には、ＭＡＣリストへの自動登録が可能となり、ユーザの負担を発生させることのないＭＡＣリスト生成が可能となる。

【０１１０】

なお、サーバにおけるＵＰｎＰプロトコルに従った処理シーケンスが的確に実行されているか否かの判定レベルとしては様々な設定が可能である。例えば、コンテンツを提供するサービスを実行するサーバにおいては、ＵＰｎＰプロトコル

に従ったコンテンツリスト要求処理、いわゆるコンテンツディレクトリサービス（ＣＤＳ）要求処理まで実行されたことを条件としてＭＡＣリストへの登録条件として設定する。

【０１１１】

すなわち、コンテンツを提供するサービスを実行するサーバにおいては、ＵＰｎＰプロトコルに従った処理シーケンス中、コンテンツリスト要求処理、いわゆるコンテンツディレクトリサービス（ＣＤＳ）要求処理が実行された場合に、サーバの保持するＭＡＣリストへの登録対象クライアントであると判定して登録処理を実行し、コンテンツディレクトリサービス（ＣＤＳ）要求処理が実行されない場合には、サーバの保持するＭＡＣリストへの登録対象クライアントではないと判定して登録処理を実行しない。

【０１１２】

このように、サーバの提供するサービスに対応するＵＰｎＰプロトコルシーケンスの実行がなされたことを条件としてＭＡＣリストへの登録を実行することにより、リスト登録の不要なクライアント機器をＭＡＣリストに登録してしまうといった無駄な登録処理を防止することができる。

【０１１３】

[識別子（ＩＤ）、鍵情報に基づく認証]

先に図４を参照して説明したように、ＭＡＣリストのクライアント登録情報には、ＭＡＣアドレス、クライアント名、登録日時の他にオプションとしてグローバルユニークな識別子としてのＧＵＩＤや、機器に対して設定された固有の鍵情報データを格納することが可能である。

【０１１４】

このようなＭＡＣアドレス以外の識別情報は、よりセキュアな管理を実現するために適用される。ＭＡＣアドレスは通常４８ビットデータであり、このデータは、一般ユーザも機器を調べることにより取得可能な情報であって基本的に秘密とされているわけではない。従って、不正を実行しようとすれば、正当なクライアント機器になりすまし、正当な機器のＭＡＣアドレスを、他の不正な機器のＭＡＣアドレスとして適用して不正機器をＭＡＣリストに登録してしまう事態も発

生しないとは言えない。

【０１１５】

比較的データ量の少ない４８ビットＭＡＣアドレスのみをクライアント確認の条件データとして適用するのではなく、さらにデータ量の多い識別データあるいは漏洩の可能性の少ないデータ等をクライアント確認のために適用することにより、高いレベルでのセキュリティ管理が実現される。

【０１１６】

登録要求を行なうクライアントは、登録処理要求パケット、またはデータ処理要求パケットのデータ部にグローバルユニークな識別子としてのＧＵＩＤ（例えば１２８ビット以上のデータ）や、機器に対して設定された固有の鍵情報データを格納し、サーバに送信する。サーバは、ＭＡＣアドレス、クライアント名、登録日時の他に、データ部に格納されたＧＵＩＤや、機器に対して設定された固有の鍵情報データを取り出してＭＡＣリストの登録情報として設定する。

【０１１７】

登録後のクライアントからのデータ処理要求において、クライアントは登録されているＧＵＩＤ、鍵情報等の識別データをパケットに格納したデータ処理要求パケットを生成してサーバに送信する。サーバは、データ処理要求パケットに含まれるＭＡＣアドレスと、ＧＵＩＤ、鍵情報等の識別データを取得して、ＭＡＣリストに登録された各データと一致するか否かを判定し、一致した場合にのみサービスを提供する。

【０１１８】

図１１を参照して、ＭＡＣアドレス以外の識別情報の照合を条件としてサービス提供を実行する場合のサーバにおける処理シーケンスについて説明する。

【０１１９】

ステップＳ５０１において、クライアントからのデータ処理要求パケットを受信すると、ステップＳ５０２において、パケットのヘッダ部に設定された送信元ＭＡＣアドレスと、データ部に格納されたＧＵＩＤ鍵情報等の識別情報を取得する。ステップＳ５０３において、パケットのヘッダ部に設定された送信元ＭＡＣアドレスと、ＭＡＣリストに登録された登録情報との照合を実行し、一致しない

場合は、未登録クライアントからの処理要求であると判定し、要求処理を実行しないで終了する。

【０１２０】

ＭＡＣアドレスの照合に成功し、一致する登録情報があった場合は、ステップＳ５０４において、パケットのデータ部に格納された識別情報と、ＭＡＣリスト中の照合ＭＡＣアドレスの格納された同一スロット中の識別情報との照合処理を実行する。

【０１２１】

識別情報が一致しない場合は、不正クライアントからの処理要求であると判定し、要求処理を実行しないで終了する。識別情報が一致した場合は、ステップＳ５０５においてクライアントの要求処理を実行する。

【０１２２】

上述した処理によれば、データ処理要求を受信したサーバが、ＭＡＣアドレスのみならず、データ量の多い識別データあるいは漏洩の可能性の少ないデータ等を用いてクライアント確認を実行することが可能となり、高いレベルでのセキュリティ管理が実現される。

【０１２３】

なお、上述の実施の形態では、ＭＡＣアドレスをクライアント識別情報として説明したが、クライアント識別情報としてＣＰＵのＩＤ、デバイスのシリアルナンバーまたはニックネーム、その他のデバイスを識別可能な情報を用いることもできる。

【０１２４】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２５】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウ

ェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１２６】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１２７】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０１２８】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０１２９】

【発明の効果】

以上、説明したように、本発明によれば、ネットワークに接続されたクライアント機器の電源をＯＮとする処理、あるいは所定アプリケーション、例えばホー

ムネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとして、ＭＡＣリスト登録処理要求パケットを自動送信し、サーバ側で、ＭＡＣリストの空きスロットの状況に応じて、受信パケットからＭＡＣアドレス等の情報を取得して登録する処理を実行する構成としたので、ユーザの負担を発生させることなくアクセス制御リストとしてのＭＡＣリストが容易に、かつ効率的に生成可能となる。

【０１３０】

また、本発明の構成によれば、サーバにＭＡＣリストの空きスロットを設定した後、閾値時間内にクライアントからの登録処理要求パケットを受信しなかった場合には、ＭＡＣリスト中の空きスロットのクローズ処理を実行する構成としたので、ＭＡＣリストの空きスロットを放置することがなくなり、サーバが第三者からの登録要求を受信した場合においても登録処理を誤って実行することがなくなり、不正なデータ処理要求に応じることが防止される。

【０１３１】

さらに、本発明の構成によれば、クライアントから受信する通常のデータ処理要求に応じてサーバ側で未登録のクライアントを登録する処理を実行する構成としたので、登録処理要求パケットを適用することなくＭＡＣリストへのクライアント登録が可能となる。

【０１３２】

さらに、本発明の構成によれば、クライアントが、特定のネットワークアクセスコントロール（ＳＮＡＣ）に従ったパケットを送信できない機器であっても、ユニバーサルプラグアンドプレイ（ＵＰｎＰ：Universal Plug and Play）対応機器であり、ＵＰｎＰプロトコルに従ったシーケンスを確実に実行している場合には、ＭＡＣリストへの自動登録が可能となり、ユーザの負担を発生させることのないＭＡＣリスト生成が可能となる。

【０１３３】

さらに、本発明の構成によれば、ＭＡＣリストの登録情報としてグローバルユニークな識別子としてのＧＵＩＤや、機器に対して設定された固有の鍵情報データを格納し、データ処理要求を受信したサーバが、ＭＡＣアドレスのみならず、

ＧＵＩＤや鍵情報等の識別データを用いてクライアント確認を実行することが可能となり、高いレベルでのセキュリティ管理が実現される。

【図面の簡単な説明】

【図１】

本発明の適用可能なネットワーク構成例を示す図である。

【図２】

ネットワーク接続機器の構成例について説明する図である。

【図３】

サーバの処理機能を説明するブロック図である。

【図４】

ＭＡＣリストの構成例について説明する図である。

【図５】

イーサネットフレームのフォーマットを示す図である。

【図６】

ＭＡＣリストに対するクライアント登録処理シーケンスを説明するフロー図である。

【図７】

ＭＡＣリスト登録要求データを説明する図である。

【図８】

ＭＡＣリストにおけるスロット設定クローズ処理について説明するフロー図である。

【図９】

データ処理要求に基づくＭＡＣリストへの登録処理を説明するフロー図である。

【図１０】

ＵＰｎＰプロトコルに従った処理シーケンスの実行を条件としたＭＡＣリストへの登録処理を説明するフロー図である。

【図１１】

ＭＡＣアドレスと他の識別情報の照合処理によるデータ処理実行可否判定を伴

うサーバの処理シーケンスを説明するフロー図である。

【符号の説明】

１００　ネットワーク

１１１　サーバ

１２１，１２２，１２４　パーソナルコンピュータ（ＰＣ）

１２３　携帯電話

１２５　ＰＤＡ

３０１　ＣＰＵ

３０２　ＲＯＭ

３０３　ＲＡＭ

３０４　ＨＤＤ

３０５　バス

３０６　入出力インタフェース

３０７　入力部

３０８　出力部

３０９　通信部

３１０　ドライブ

３１１　リムーバブル記録媒体

５０１　パケット送受信部

５０２　パケット生成、解析部

５０３　登録可否判定部

５０４　登録処理部

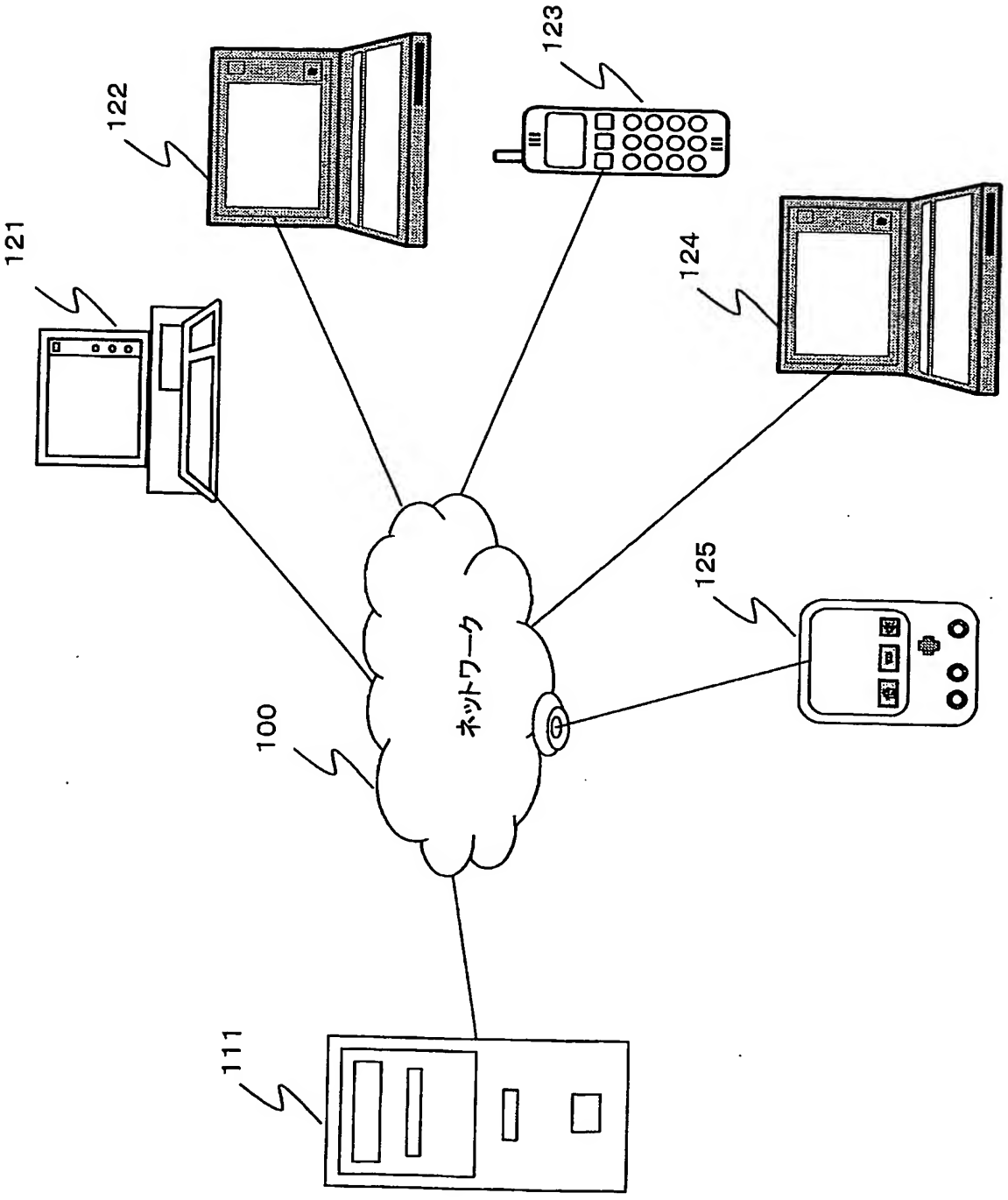
５０５　記憶部

５０６　データ処理可否判定部

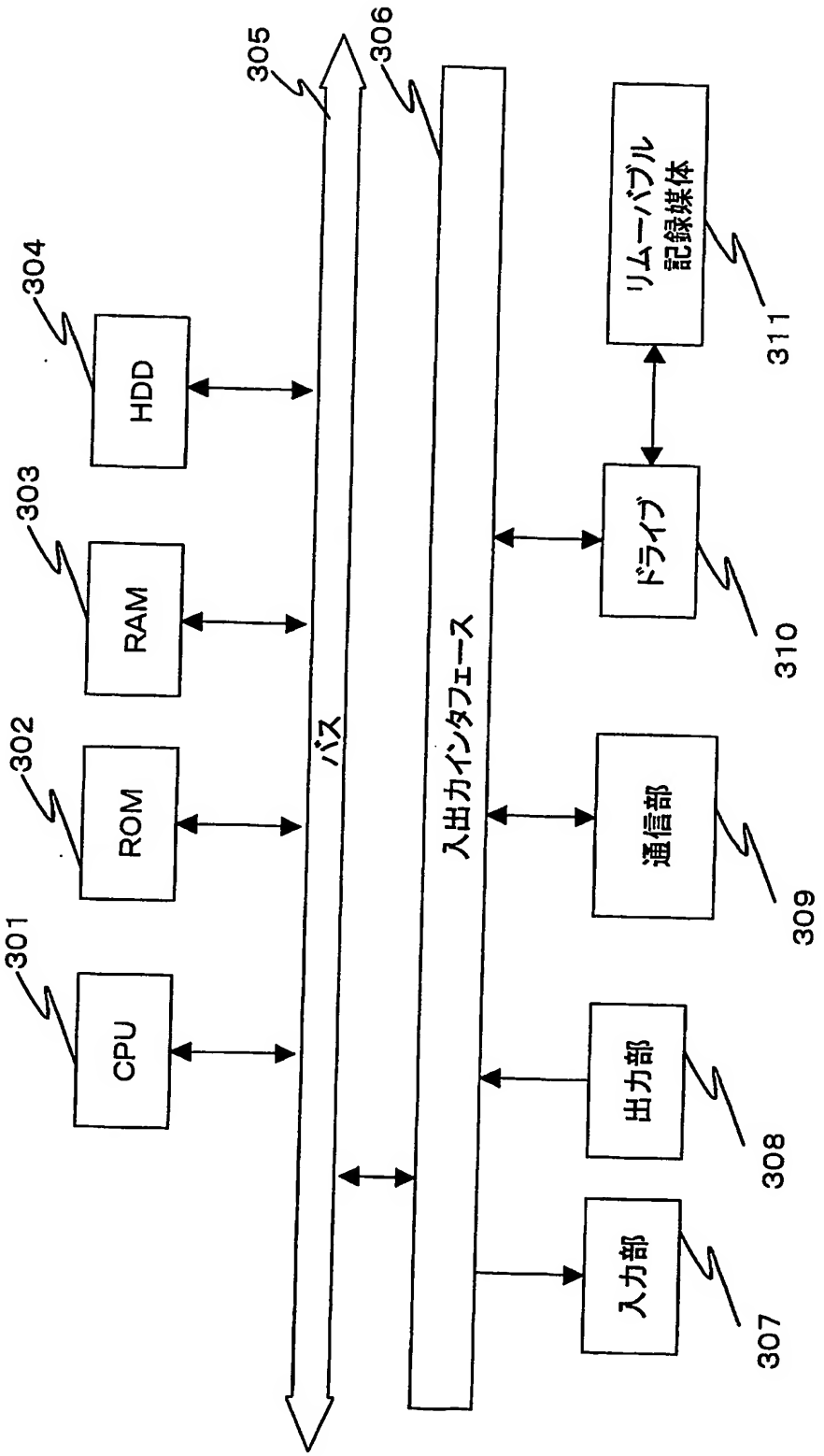
５０７　データ処理部

【書類名】　図面

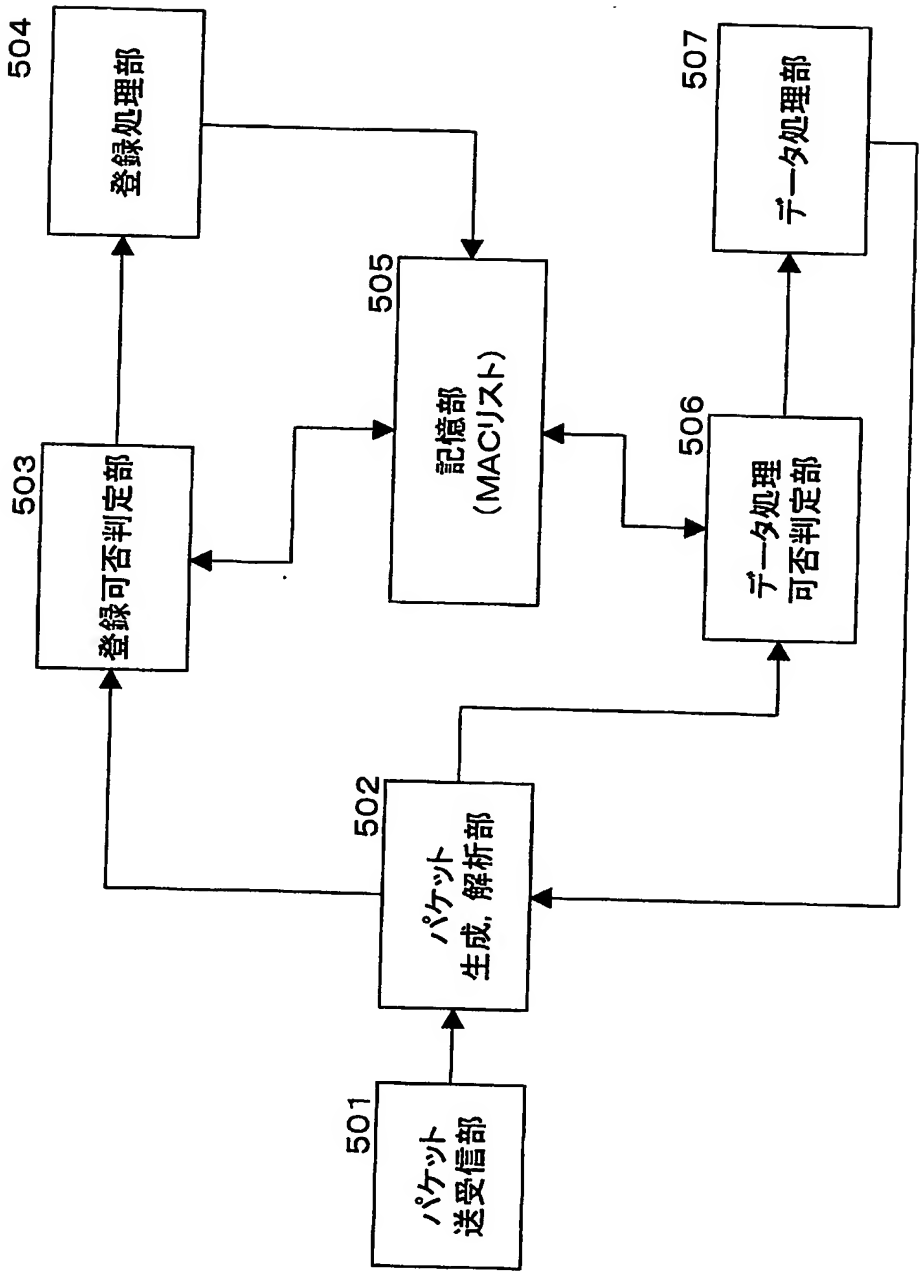
【図１】



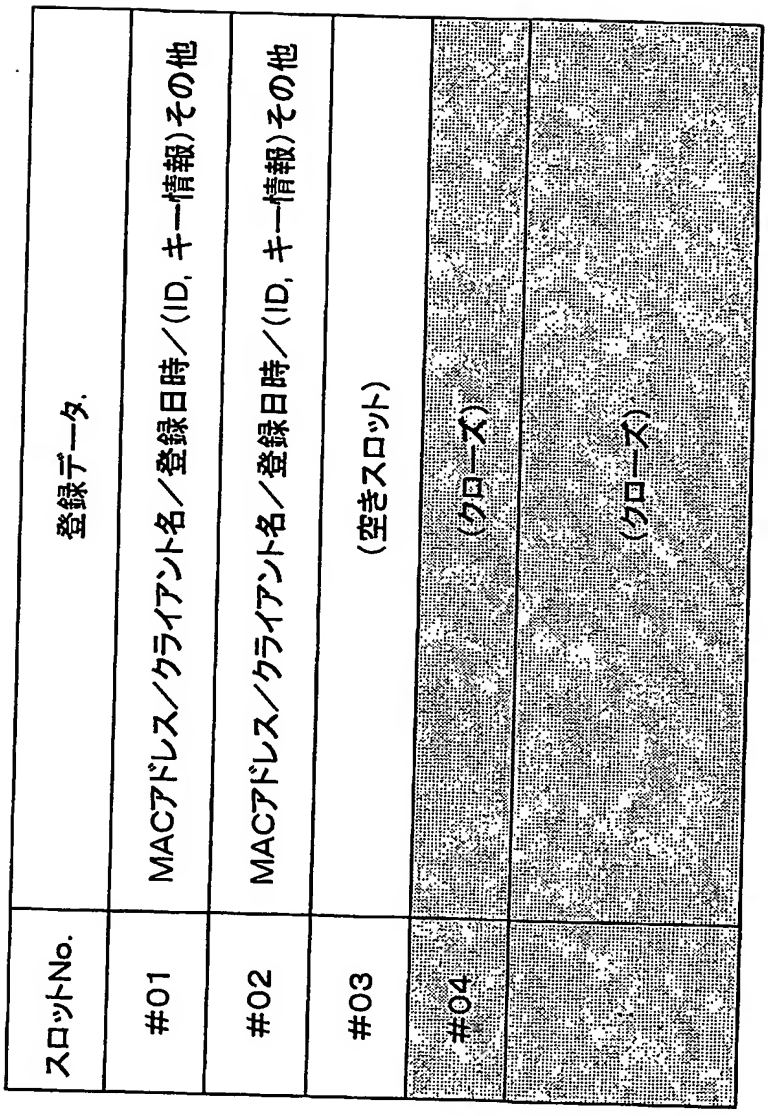
【図２】


305
306
304
HDD
303
RAM
302
ROM
301
CPU
バス
入出力インタフェース
リムーバブル
記録媒体
311
ドライブ
310
通信部
309
出力部
308
入力部
307

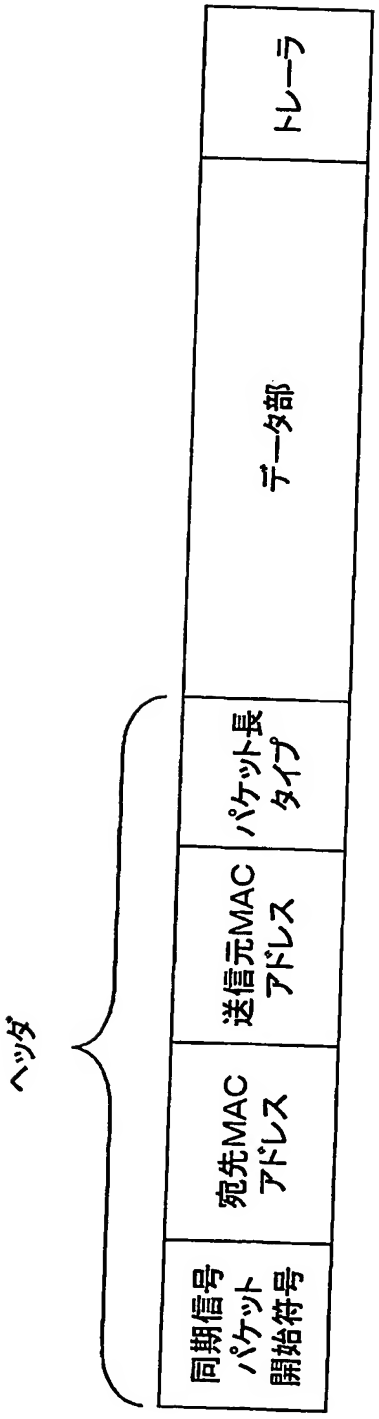
【図３】


504
登録処理部
507
データ処理部
505
記憶部
(MACリスト)
503
登録可否判定部
506
データ処理
可否判定部
502
パケット
生成，解析部
501
パケット
送受信部

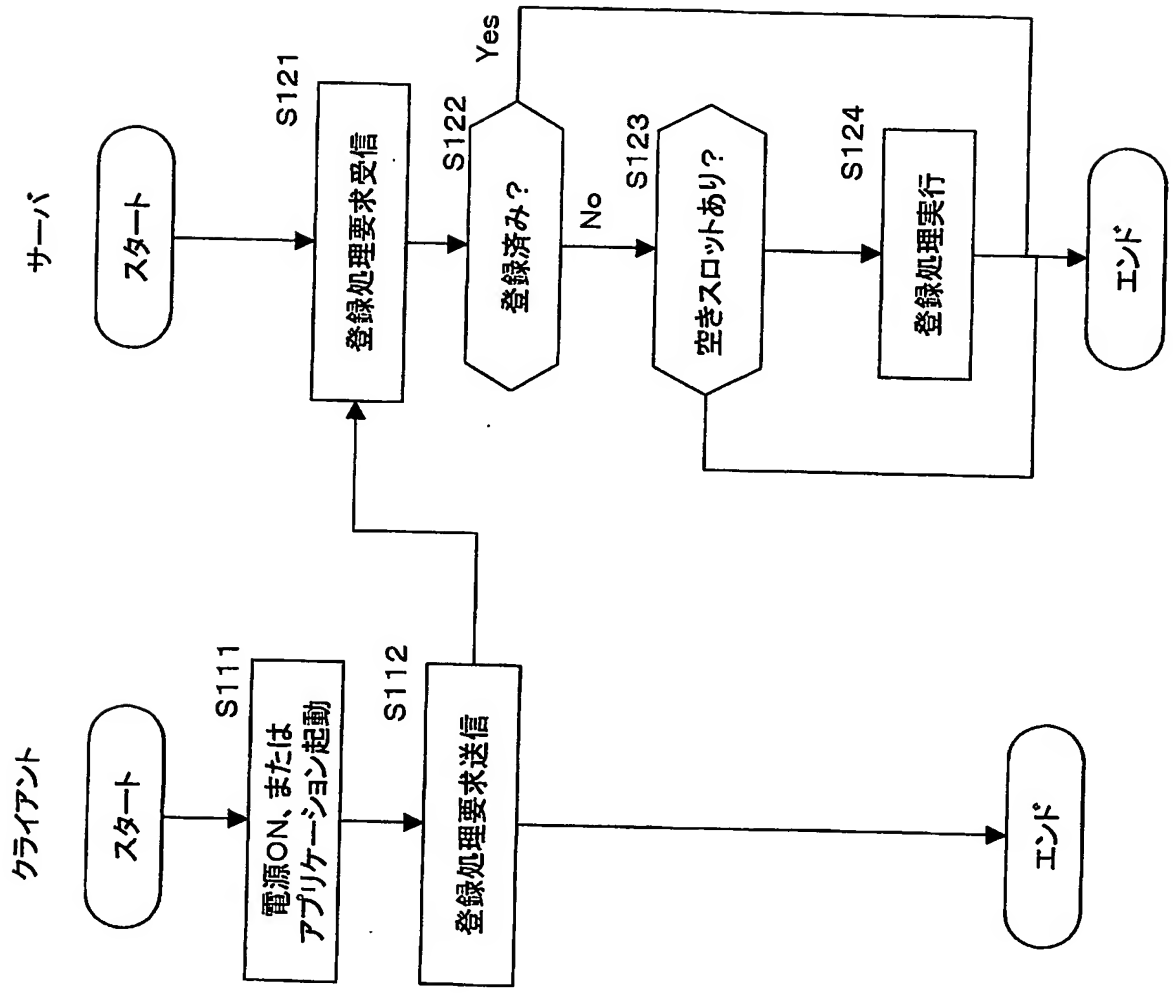
【図４】


スロットNo.
登録データ
#01
MACアドレス／クライアント名／登録日時／(ID, キー情報)その他
#02
MACアドレス／クライアント名／登録日時／(ID, キー情報)その他
#03
(空きスロット)
#04
(クローズ)
(クローズ)

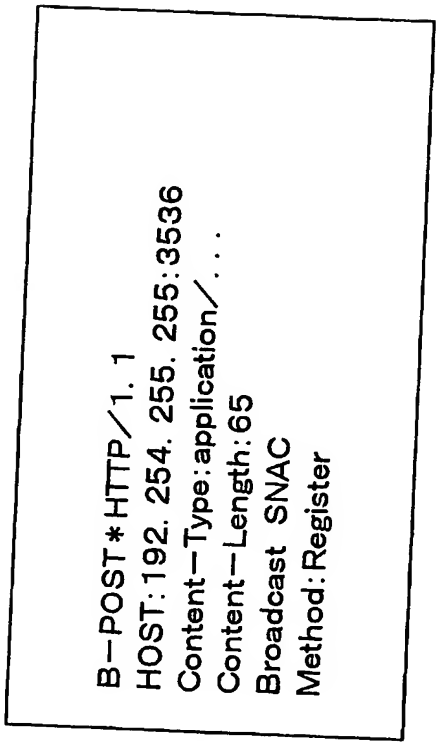
【図５】


ヘッダ
同期信号
パケット
開始符号
宛先MAC
アドレス
送信元MAC
アドレス
パケット長
タイプ
データ部
トレーラ

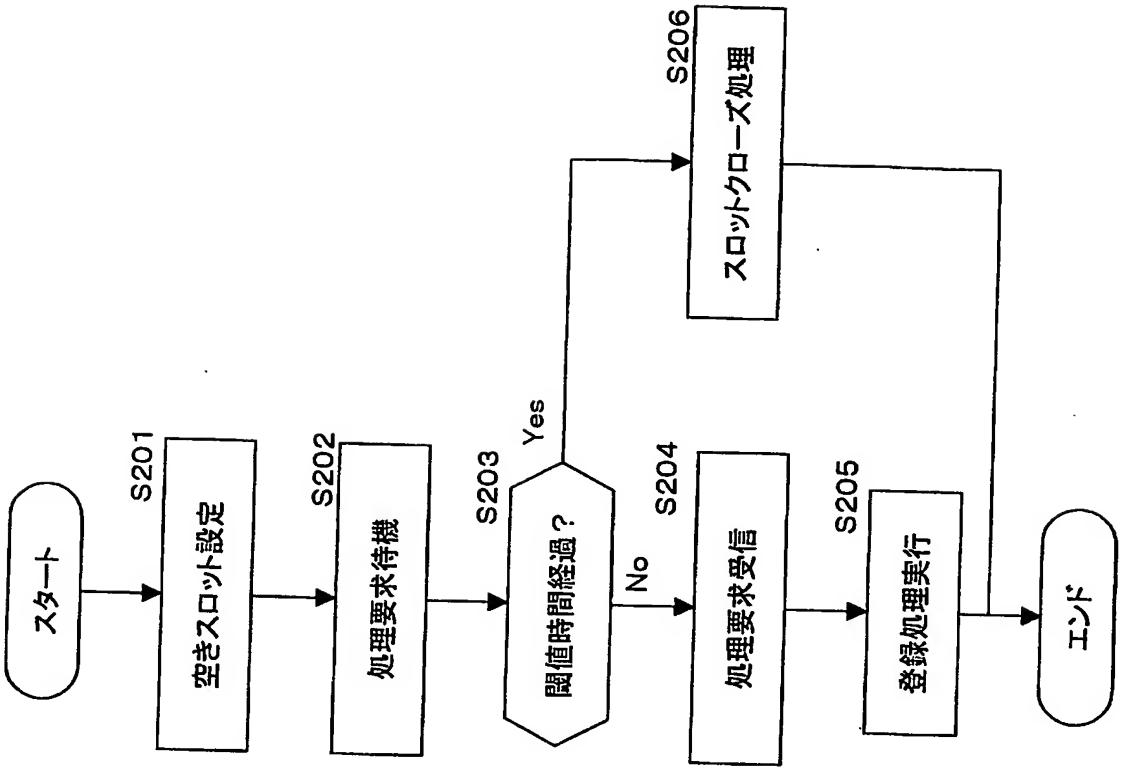
【図６】


サーバ
スタート
S121
登録処理要求受信
S122
登録済み？
Yes
No
S123
空きスロットあり？
S124
登録処理実行
エンド
クライアント
スタート
S111
電源ON、またはアプリケーション起動
S112
登録処理要求送信
エンド

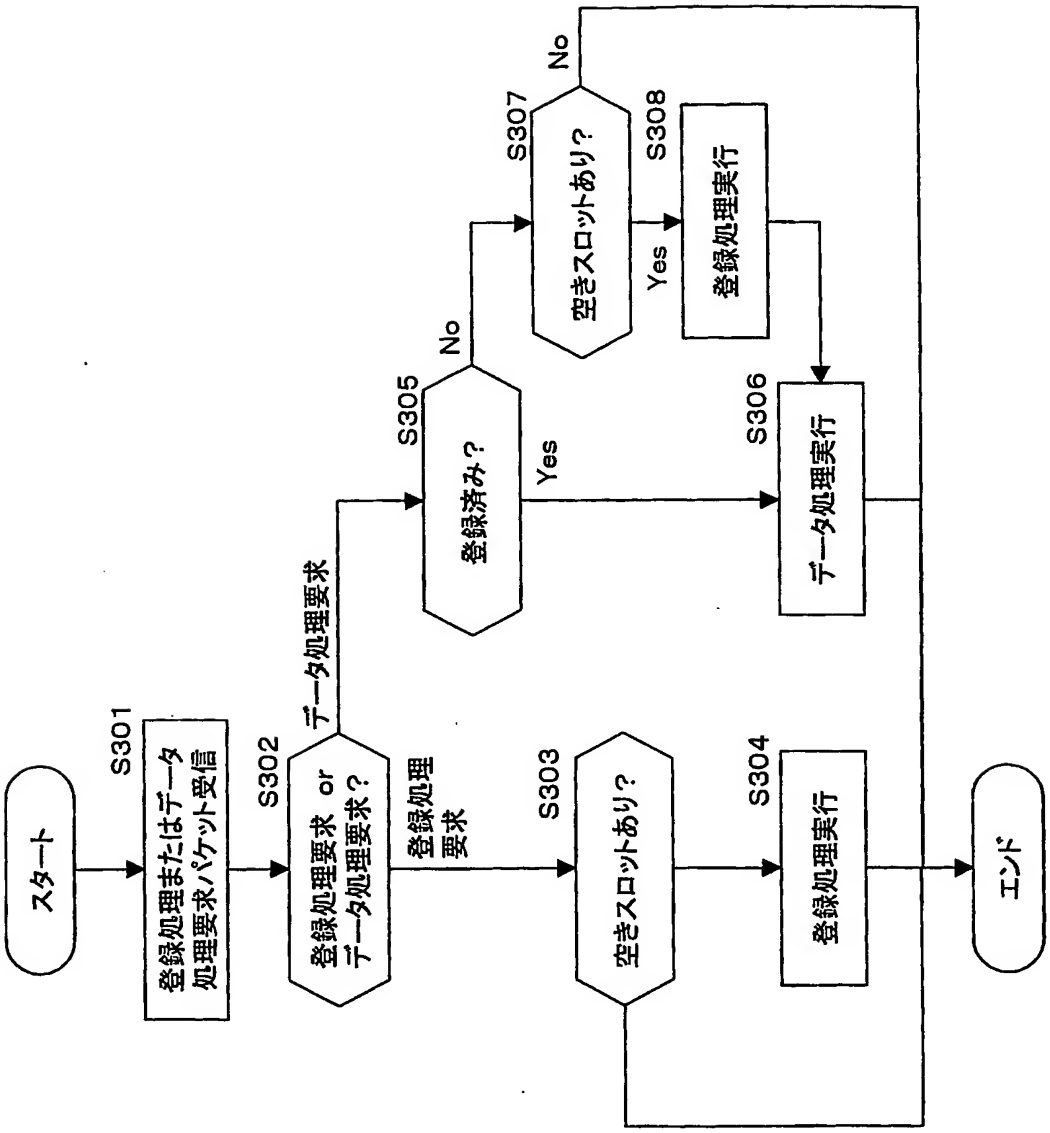
【図７】


B－POST＊HTTP／1．1
HOST：192．254．255．255：3536
Content－Type：application／．．．
Content－Length：65
Broadcast SNAC
Method：Register

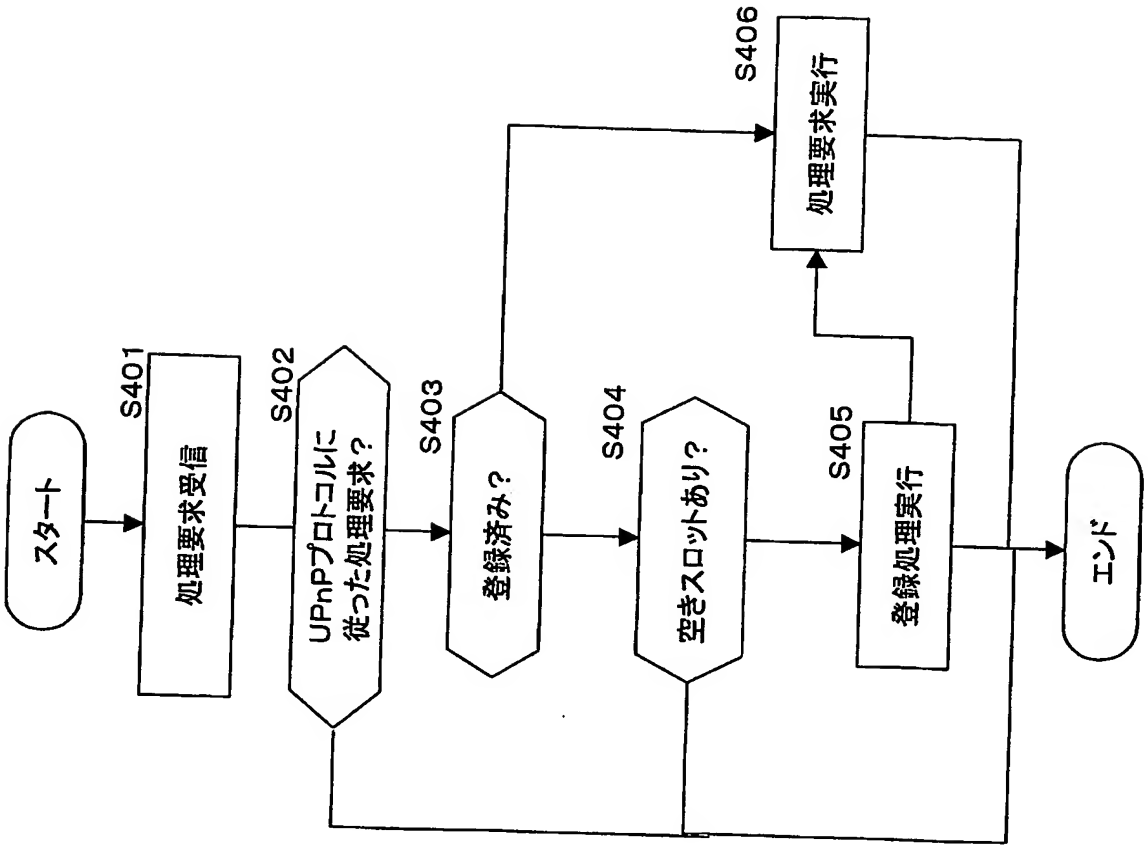
【図８】


スタート
S201
空きスロット設定
S202
処理要求待機
S203
閾値時間経過？
Yes
No
S204
処理要求受信
S205
登録処理実行
S206
スロットクローズ処理
エンド

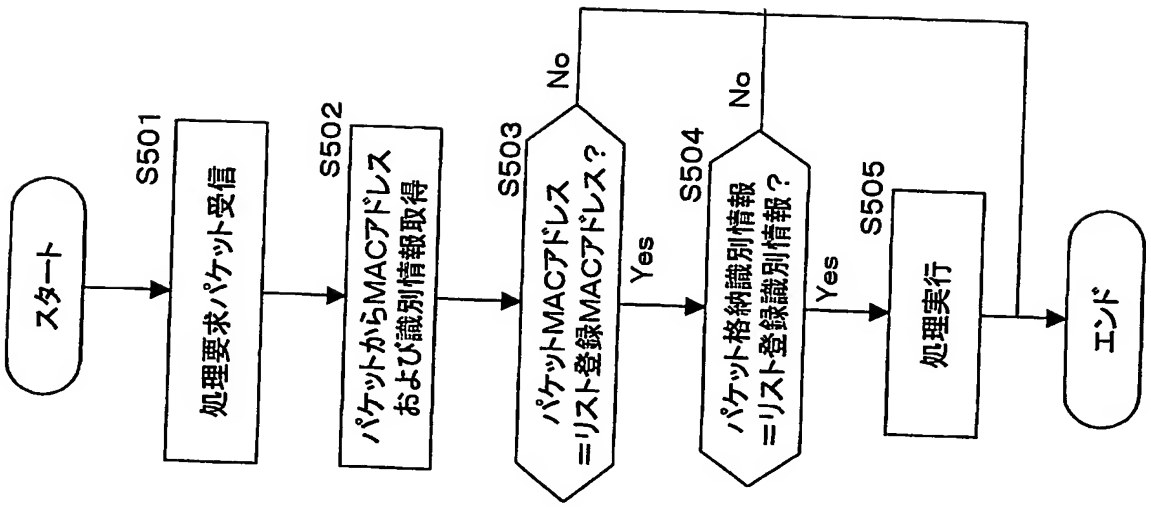
【図９】


スタート
S301
登録処理またはデータ処理要求パケット受信
S302
登録処理要求 or データ処理要求?
データ処理要求
登録処理要求
S303
空きスロットあり?
S304
登録処理実行
エンド
S305
登録済み?
No
Yes
S306
データ処理実行
S307
空きスロットあり?
No
Yes
S308
登録処理実行

【図１０】


スタート
S401
処理要求受信
S402
UPnPプロトコルに
従った処理要求？
S403
登録済み？
S404
空きスロットあり？
S405
登録処理実行
S406
処理要求実行
エンド

【図１１】


スタート
S501
処理要求パケット受信
S502
パケットからMACアドレス
および識別情報取得
S503
パケットMACアドレス
=リスト登録MACアドレス？
No
Yes
S504
パケット格納識別情報
=リスト登録識別情報？
No
Yes
S505
処理実行
エンド

【書類名】　要約書

【要約】

【課題】　アクセス制御リストとしてのＭＡＣリストの生成をユーザに負担を強いることなく効率的に生成する装置および方法を提供する。

【解決手段】　ネットワークに接続されたクライアント機器の電源ＯＮ処理、あるいは所定アプリケーション、例えばホームネットワークを利用したサービスの実行アプリケーションを起動する処理のいずれかの処理をトリガとしてＭＡＣリストに対する登録処理要求パケットを自動送信する。サーバは、ＭＡＣリストの空きスロットの状況に応じて、受信パケットからＭＡＣアドレス等の情報を取得して登録処理を実行する。本構成により、ユーザの負担を発生させることなくアクセス制御リストとしてのＭＡＣリストが容易に確実に生成可能となる。

【選択図】　図６

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社